UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MISSOURI EASTERN DIVISION

UNITED STATES OF AMERICA,)
Plaintiff,))
vs.) Case No. 4:09CR506DJS(MLM)
MICHAEL R. MASSEY,)
Defendant.)

REPORT AND RECOMMENDATION OF UNITED STATES MAGISTRATE JUDGE

This matter is before the court on defendant's Motion to Suppress Evidence and Statements. [Doc. 12] The government responded. [Doc. 13] Defendant replied. [Doc. 14] The government sur-replied. [Doc. 19] An Evidentiary Hearing was held on September 3, 2009. Defendant appeared in person and by counsel, Mr. Murry A. Marks. The government was represented by Assistant United States Attorney Carrie Costantin. The government presented the testimony of Detective Michael McCartney of the St. Louis County Police Department. Defendant did not present evidence. Based on the testimony and evidence adduced and having had an opportunity to observe the demeanor and evaluate the credibility of the witness, the undersigned makes the following findings of fact and conclusions of law.

FINDINGS OF FACT

Detective Michael McCartney testified he is employed by the St. Louis County Police Department. He has been a police officer for 15 years. He is currently assigned to the Division of Criminal Investigation/Special Investigations Unit. He described his training: attendance at IT classes, investigative classes concerning crimes against children over the computer and national conferences concerning the Internet and child pornography.

On June 23, 2008 Det. McCartney presented an Application for a Search Warrant for 7378 Hazel Avenue with an 8 page Affidavit in Support to the Honorable John Ross of the St. Louis County Circuit Court.

The Affidavit in Support states that he has reason to believe that evidence of:

POSSESSION OF CHILD PORNOGRAPHY to wit TO SEIZE, SEARCH AND ANALYZE ANY AND ALL ELECTRONIC DATA PROCESSING AND STORAGE DEVICES, COMPUTERS AND COMPUTER SYSTEMS INCLUDING CENTRAL PROCESSING UNITS, INTERNAL PERIPHERAL STORAGE DEVICES SUCH AS FIXED DISKS. EXTERNAL HARD DISKS. FLOPPY DISKS AND DISKETTES, TAPE DRIVES AND TAPES, OPTICAL STORAGE DEVICES OR OTHER MEMORY STORAGE DEVICES. PERIPHERAL INPUT/OUTPUT DEVICES SUCH AS KEYBOARDS, PRINTERS. VIDEO DISPLAY MONITORS. OPTICAL READERS AND RELATED COMMUNICATIONS DEVICES SUCH AS MODEMS, ROUTERS AND OTHER WIRELESS DEVICES; ANY AND ALL CAMERAS AND RELATED EQUIPMENT, VIDEO AND AUDIO RECORDERS AND ALL RELATED RECORDING EQUIPMENT. ANY AND ALL PHOTOGRAPHS, COPIES OF PHOTOGRAPHS AND ANY MANUFACTURED HARD COPY OF IMAGES RELATED TO CHILD PORNOGRAPHY. ANY AND ALL LOGS CONTAINING USER NAMES, PASSWORDS AND DOCUMENTATION OR OTHER IDENTIFIERS NECESSARY TO EXAMINE OR OPERATE ITEMS. TOGETHER WITH SYSTEM DOCUMENTATION, OPERATING LOGS AND HAND WRITTEN NOTES RELATED TO USER IDENTIFICATIONS. PASSWORDS AND/OR CHILD PORNOGRAPHY

would be found at the 7378 Hazel address. The residence is described with particularity. The Affidavit goes on to describe Det. McCartney's experience including contacts with informants and other police officers and subjects known to possess child pornography. It describes his training as having attended courses relating to child pornography and computer technology including but not limited to Internet Crimes Against Children (ICAC), Task Force Investigative Techniques Training and the fact that he has attended the ICAC training seminar relating to child exploitation. He has also been trained in the Knoppix computer scan and has attended 36 hours training in undercover computer chatting.

The Affidavit states that the matters contained in the Affidavit are based on Det.

McCartney's personal knowledge or information provided to him by other law enforcement

officers. It says that because the Affidavit is being submitted for the limited purpose of securing a search warrant, the Affidavit has not included each and every fact known to the affiant concerning the investigation.¹

The Affidavit states that on June 17, 2008, Det. McCartney was notified by Sgt. Adam Kavanaugh of the St. Louis County Police Department that during an authorized Internet undercover operation conducted on May 13, 2008 at 01:15 hours, a computer in the State of Missouri was identified as offering to participate in the distribution of child pornography.² The Affidavit states that while using software configured to search the Gnutella Network (a public file sharing network) for IP addresses that had previously been identified through investigative techniques as possessing or offering to share, files known to law enforcement that contain images/videos of child pornography, Sgt. Kavanaugh was able to identify a computer using the IP address of 68.188.82.208, in the St. Louis, Missouri area. Aff. § 5.

Sgt. Kavanaugh directly connected and successfully browsed a computer located at the IP address of 68.188.82.208 and obtained a list of publicly available files. He was able to identify the files by their SHA1 value which he had previously seen during prior investigations and believed to be child pornography. Aff. ¶ 6.

The entire Affidavit contains the probable cause for the issuance of the Search Warrant. The Affidavit is incorporated by reference as if fully set out herein. It is summarized here merely to assist the district court.

The Affidavit describes Sgt. Kavanaugh's training and experience as well. It states that he has been a Police Officer for approximately 15 years; that he is the Supervisor of the Special Investigations Unit for the St. Louis County Police Department's Division of Criminal Investigations; that he has training through the Internet Crimes Against Children Task Force in the area of child pornography and investigations; that he is trained in the use of the Peer Precision Investigative Tool; and he has been to the National Center for Missing and Exploited Children for supervisory training in the area of child pornography. Aff \P 3.

The Affidavit then describes by file name, SHA1 number and a brief narrative each of the 26 files identified which all depict minors engaged in sexually explicit conduct. The Affidavit notes that the list of files is merely a partial list. Aff. ¶ 6.

On June 19, 2008 Det. McCartney viewed the files and found them to contain the images as described. Aff. \P 7.

A subpoena dated May 13, 2008 was sent to Charter Communications for the name, address and billing information on the IP address of 68.188.82.208 assigned on May 13, 2008 at 01:15:19 hours. Sgt. Kavanaugh received a response from Charter Communications dated June 3, 2008 advising that the IP address was assigned to Ken Massey, 7378 Hazel Avenue, Maplewood, Missouri 63143 with a billing telephone number of 314-645-4117. Aff. ¶8.

An Ameren UE utilities check revealed that 7378 Hazel Avenue, Maplewood, Missouri 63143 has been registered to Kenneth R. and Margeret Massey since April 2, 2002 with a telephone number of 314-517-1488. Kenneth R. Massey's Social Security number is listed in the Affidavit. Aff. \P 9.

Det. McCartney stated that he knew from his training, experience and the information provided by Sgt. Kavanaugh that the search results indicated that a computer using the IP address of 68.188.82.208 possessed and/or contributed to the distribution of child pornography . Aff. \P 10.

Peer Precision Training specifically deals with the use of a publicly available Gnutella network through a publicly available Gnutella client (software by which one accesses the Gnutella network) and SHA1 values. These SHA1 values are gathered by the National Center for Missing and Exploited Children and various nationwide law

enforcement agencies to locate computers distributing in part, images believed to be child pornography. Aff. ¶ 11.

Det. McCartney stated that he knew from his training and experience that digital files can be processed by this SHA1 process resulting in a digital signature. By comparing these signatures, one can conclude that two files are identical with a precision that greatly exceeds 99.9% certainty based on information from the National Institute of Standards and Technology. Aff. \P 12.

Det. McCartney knew from his training and experience that Internet computers identify each other by an Internet Protocol or IP address. He knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet. Aff. ¶ 13.

Det. McCartney knew from his training and experience that searching on the Gnutella Peer-to-Peer network can result in Sgt. Kavanaugh receiving lists of addresses identifying locations where a computer has Gnutella software installed and individual files have been reported as available for download with a specific digital structure. Aff. ¶ 14.

Det. McCartney knew from his training and experience that by examining a list of IP addresses Sgt. Kavanaugh can locate computers that are reported to be in Missouri as well as other states. By comparison of the SHA1 digital signatures, Det. McCartney could conclude that a computer, originating from an IP address known to be in Missouri, has Gnutella or comparable software installed on it and contains specific and known images of child pornography. The SHA1 value for a file will remain the same unless the file has been changed in any way. Then a different SHA1 value would be assigned to the file. Aff.¶ 15.

Det. McCartney knew from his training and experience that persons trading in, receiving, manufacturing, distributing or possessing images of the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of persons interested in child pornography or child exploitation. Aff. ¶ 16.

Det. McCartney knew from his training and experience that computers used to access the Internet usually contain files, logs or remnants which would tend to show ownership and use of the computer as well as ownership and use of the Internet service accounts used for the Internet access. Aff. ¶ 17.

Det. McCartney knew from his training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files. Aff. ¶ 18.

Det. McCartney knew from his training and experience that people who collect child pornography tend to keep images they get for extended periods of time and do not delete the images. They tend to regard the images as trophies and use them for sexual gratification. They also use them as bargaining tools when trading with others. Aff. ¶ 19.

Det. McCartney knew from his training and experience that people who tend to collect images of child pornography use video and audio components to capture and record child pornography. They are also known to transfer these images to other digital media storage devices. Aff. ¶ 20.

Based on the contents of the Application and Affidavit, Judge Ross found there was probable cause to believe that child pornography would be found at 7378 Hazel Avenue in

Maplewood, Missouri and he issued a Search Warrant for that address to seize and search and analyze any and all of the items set out in capital letters on page 2 in this Report & Recommendation. Gov.Ex.1.

Det. McCartney testified that the Search Warrant was executed on June 26, 2008. Pursuant to standard practice for the execution of all county search warrants, entrance was made by the County Tactical Operations Unit. According to procedure, they enter a residence, secure it and then call the detectives to conduct the search. While the residence on Hazel was being secured, three people walked down the street towards the house. They were stopped and identified themselves as Mr. and Mrs. Kenneth Massey and their daughter. Det. McCartney spoke to Mrs. Massey and told her they were executing a search warrant for child pornography. Mrs. Massey said she lived in the residence with her husband, her daughter, her son Michael, and Michael's friend, Norman Parham. She said she thought Michael and Norman were present in the residence.

The Tactical Unit brought out two individuals who were located in the house. They were handcuffed for the officers' safety. Det. McCartney spoke to defendant Michael Massey. He took him to the rear of the house and removed the handcuffs. Defendant was wearing a t-shirt and boxer shorts. Someone brought him a pair of pants and Det. McCartney allowed him to put them on.

Det. McCartney introduced himself to defendant and told him they were executing a search warrant for child pornography. Defendant said he lived in the residence with his mother, father, sister and Norman Parham. Det. McCartney said he would like to ask defendant some questions and he advised him of his Miranda rights. The advice was done orally. He told him he had the right to remain silent, that is, to say nothing. He told him that anything he said would be used against him; he had the right to have an attorney

present for any questioning and if he could not afford an attorney one would be appointed for him. Defendant indicated he understood his rights and said he was willing to answer questions.

Defendant said he had a computer; in fact, each person in the residence had a computer. He said he used a file sharing program called LimeWire.³ He asked what the search warrant was for and Det. McCartney told him again it was for child pornography. Defendant said "It's all mine, all the child porn is on my computer."

Det. McCartney told defendant to hold off making any more statements until he could further investigate at department headquarters. Det. McCartney told defendant he was not under arrest. He told him if he participated at Headquarters it would be completely voluntary.

Defendant said he would cooperate and Det. McCartney drove defendant to Headquarters. Defendant was not handcuffed. During the drive there was no discussion about the investigation.

In <u>United States v. Stults</u>, 575 F.3d 834 (8th Cir. 2009), 2009 WL 2476695 (8th Cir. 8/14/09) LimeWire is described:

[&]quot;LimeWire is a peer-to-peer file sharing application that connects users who wish to share data files with one another." <u>United States v. Lewis</u>, 554 F.3d 208, 211 (1st Cir. 2009). It is "indifferent to the nature of the data-images or text or music or video or software. [It is] equally indifferent to the legal status of the data-public-domain or copyrighted or contraband." <u>Id.</u> "LimeWire combines two functions: the ability to search for and download files from other users and the ability to make files on one's own computer available to other users." <u>Id.</u> When a user wants to download files from other users, he "launches LimeWire and inputs a search term or terms. The application then seeks matches for those terms in the file names and descriptions of all files designated for sharing on all computers then running the LimeWire application. . . ." <u>Id.</u> LimeWire will then "display [] a list of file names that match the search terms and the user can select one or more of those to begin downloading the files." <u>Id.</u>

They went to an interview room in the Criminal Investigations Unit offices. Det. McCartney activated an audio recorder. The first 6 minutes of the recording were played during the Evidentiary Hearing (Gov.Ex.3) and it shows clearly that the defendant had been advised of his Miranda rights and specifies that the defendant was there voluntarily and that he had come to the office with Det. McCartney but that no discussion had taken place during the trip. It shows he was re-advised of his rights and that he signed the Waiver form. (Gov.Ex.2) It shows, and Det. McCartney testified, how he re-advised defendant of his rights: he read each right to defendant and defendant initialed that he understood. Defendant then read the Waiver out loud. Det. McCartney told him if he wanted to speak, to sign the form and if he did not want to speak, not to sign the form.

The interview is in four parts (at one point, the battery on the recorder died).

Defendant made incriminating statements about possessing child pornography. <u>See</u>

Gov.Ex.3.

CONCLUSIONS OF LAW

Probable Cause

Defendant first argues that the Search Warrant lacked probable cause because the only link between the defendant's residence and the child pornography observed by Sgt. Kavanaugh was the IP address 68.122.82.208. Defendant contends the Affidavit was defective because it could not specify which computer had the child pornography, that a person could have used the IP from outside the residence if there was a wireless network at the residence and that a person could have used a proxy server to create a fake IP address.

Search warrants to be valid must be based on a finding by a neutral detached judicial officer that there is probable cause to believe that evidence, instrumentalities or fruits of

a crime, contraband or a person for whose arrest there is probable cause may be found in the place to be searched. Johnson v. United States, 333 U.S. 10 (1948); Warden v. Hayden, 387 U.S. 294 (1967); Fed.R.Crim.P. 41. The standard of probable cause for the issuing judge is whether, given the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). Probable cause is "a fluid concept--turning on the assessment of probabilities in particular factual contexts--not readily, or even usefully, reduced to a neat set of legal rules." Gates, 462 U.S. at 232. Applications and affidavits should be read with common sense and not in a grudging, hypertechnical fashion. United States v. Ventresca, 380 U.S. 102, 109 (1965). Information contained in applications and affidavits for search warrants must be examined in the totality of the circumstances presented. Gates, 462 U.S. at 230. The duty of the reviewing judge "is simply to ensure that the [issuing judge] had a `substantial basis for . . . conclud[ing]' that probable cause existed." Gates, 462 U.S. at 238-39, quoting Jones v. United States, 362 U.S. 257, 271 (1960). Once a judicial officer has issued a warrant upon a finding of probable cause, that finding deserves great deference. Gates, 462 U.S. at 236. The Affidavit presented in the instant case clearly contains the "fair probability" that evidence, instrumentalities or fruits of a crime or contraband would be found at 7378 Hazel. The facts set out above show that there was a substantial basis for concluding that probable cause existed.

In <u>United States v. Solomon</u>, 432 F.3d 824, 827 (8th Cir. 2005) the Eighth Circuit held that when the issuing judge relies solely on a supporting affidavit to issue a warrant "only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause", <u>quoting United States v.</u> Etheridge, 165 F.3d 655, 656 (8th Cir. 1999), quoting United States v. Gladney, 48 F.3d 309,

312 (8th Cir. 1995); <u>United States v. Wells</u>, 347 F.3d 280, 286 (8th Cir. 2004) (when issuing court relies solely on an affidavit to determine whether probable cause exists, only the information found within the four corners of the affidavit may be considered by reviewing court).

The Search Warrant at issue in this case established that there was probable cause to believe that child pornography was on a computer located at defendant's residence. Sgt. Kavanaugh determined that there were at least 26 files of known child pornography on a computer using the IP address of 68.188.82.208 on May 13, 2008 at 1:15:19. The Internet Service Provider's records indicated that the IP address was assigned to defendant's residence on that date and time. The Search Warrant was for the residence and all computers therein. Defendant's argument that the Affidavit was defective because it could not specify which computer had the child pornography is not well taken. The Affidavit established that there was probable cause to believe that a computer at the defendant's residence had child pornography on it. The Search Warrant properly sought to search the residence and all computers in the residence.

In <u>United States v. Perez</u>, 484 F.3d 735 (5th Cir. 2007), the court rejected an argument similar to the one raised by defendant in the present case that is, that the connection between and IP address and a physical address was insufficient probable cause to search a residence for child pornography:

<u>Perez</u> argues that the association of an IP address with a physical address does not give rise to probable cause to search that address. He argues that if he "used an unsecure wireless connection, then neighbors would have been able to easily use [Perez's] Internet access to make the transmissions." But though it was possible that the transmissions originated outside of the residence to which the IP address assigned, it remained likely that the source of the transmissions was inside that residence. <u>See United States v. Grant</u>, 218 F.3d 72, 73 (1st Cir. 2000) (stating that "even discounting for the possibility that an individual other than [defendant] may have been using his account, there was a *fair probability* that [defendant] was the user and that

evidence of the user's illegal activities would be found in [defendant's] home") (emphasis in original). "[P]robable cause does not require proof beyond a reasonable doubt." <u>United States v. Brown</u>, 941 F.2d 1300, 1302 (5th Cir. 1991).

This reasoning refutes defendant's argument in the instant case. It is possible that the person sharing child pornography was actually wirelessly accessing defendant's IP address or that such person used a proxy server that randomly generated defendant's IP address, there was still a *fair probability* that a person at defendant's residence was the user and the child pornography would be found in defendant's home.

Numerous other districts have found that probable cause supports the issuance of a search warrant when the investigation links child pornography to an IP address and the IP address is subsequently tied to a specific residence. See United States v. Latham, 2007 WL 4563459 (D.Nev. 2007) (unreported) (peer-to-peer file sharing investigation); United States v. Courtney, 2008 WL 4998997 (E.D.Ark. 2008) (unreported) (agent downloaded child pornography from IP address); United States v. Carter, 549 F.Supp. 1257, 1269 (computer at IP address attempted to download child pornography from undercover agent); United States v. Merz, 2007 WL 1183771 (E.D.Pa. 2009) (unreported) (computer at IP address attempted to download child pornography from undercover agent). See also United States v. Cartier, 543 F.3d 442, 446-47 (8th Cir. 2008), in which the court found that probable cause existed to issue a search warrant for defendant's residence where the affidavit described an undercover peer-to-peer file sharing investigation in which the Spanish police had observed files on a computer at a certain IP address and had hash values identical to known child pornography files and the IP address for that time came back to an account at the defendant's residence.

Defendant asserts that <u>Perez</u> should be distinguished because the user of the IP address in <u>Perez</u> had a password-protected Yahoo account which would have strengthened

probable cause. In Perez a woman complained to the police that she had received an Internet message from someone with the Yahoo ID "famcple," who proceeded to show her images of young children engaged in sexual acts. Her complaint was forwarded to the Buffalo, New York division of the FBI which sent a subpoena to Yahoo! Incorporated ("Yahoo") seeking information regarding the user of Yahoo ID "famcple." Yahoo responded that the user's login name was "stephenmee2003," and that the user's full name was "Mr. Rob Ram," and noted that on the dates when the child pornography was transmitted the user had a specific IP address. The FBI determined that the owner of the IP address was Time Warner Cable ("Time Warner"). After being served with a subpoena Time Warner informed the FBI that the IP address in question was assigned to Javier Perez, residing at 7608 Scenic Brook Drive, Austin, Texas 78736. The FBI sought a warrant to search the address. Just as in the present case, defendant argued that another person perhaps "Stephen Mee" or "Mr. Rob Ram" had accessed his wireless Internet connection and used it to send the child pornography. In other words, the fact that the Yahoo account that sent the child pornography was password-protected provided no additional indicia of reliability - - in fact it cut the other way - - specifically that Mr. Rob Ram might have been using defendant's unsecured wireless connection. However, as noted above, the court rejected this argument and held that probable cause existed to determine that the child pornography had been transmitted from defendant's residence.

In the present case the Search Warrant Affidavit stated that Sgt. Kavanaugh observed more than 20 files of child pornography on a computer using the IP address that was issued to defendant's residence. The child pornography was actually seen on a computer using an Internet connection at defendant's residence. There was clearly

probable cause to find that child pornography would be at the residence and defendant's Motion should be denied.

Particularity

Defendant agues that the Search Warrant in this case violates the particularity requirement of the Fourth Amendment. He argues that the Warrant allows a search of all personal and private information having nothing to do with child pornography, the very type of "fishing expedition" forbidden by the Fourth Amendment. Defendant's argument is without merit.

A search warrant must describe with particularity the place to be searched and the things to be seized. U.S. Const. Amend. IV; Rule 41, Federal Rules of Criminal Procedure. Police officers executing a search warrant may search for and seize items described in the search warrant. They may also seize other items of evidence, contraband or instrumentalities of a crime if discovered during the reasonable course of the search. Warden v. Hayden, 387 U.S. 294, 298-301 (1967); United States v. Peterson, 867 F.2d 1110, 1112-14 (8th Cir. 1989). The discovery of such other items need not be "inadvertent." See Horton v. California, 496 U.S. 128, 110 S.Ct. 2301, 2308-11 (1990).

The degree of particularity required is flexible and may vary depending on the circumstances and the type of items involved. <u>United States v. Horn</u>, 187 F.3d 781, 788 (8th Cir. 1999); <u>United States v. Muckenthaler</u>, 584 F.2d 240, 245 (8th Cir. 1978). <u>See also United States v. Dennis</u>, 625 F.2d 782, 792 (8th Cir. 1980) (search warrant for "certain books and records (or items of evidence) relating to the extortionate credit transaction business" held valid). "[W]here the precise identity of goods cannot be ascertained at the time the warrant is issued naming only the generic class of items will suffice because less particularity can be reasonably expected than for goods (such as those stolen) whose exact

identity is already known at the time of issuance." <u>Dennis</u>, 625 F.2d at 792, <u>quoting United States v. Johnson</u>, 541 F.2d 1311, 1314 (8th Cir. 1976); <u>see also United States v. Coppage</u>, 635 F.2d 683, 687 (8th Cir. 1980) (warrant found valid which authorized search for "books, records, chemical equipment, and personal papers relating to the manufacture and distribution of methamphetamine").

The Fourth Amendment requires that Search Warrants describe the things to be seized with sufficient particularity to prevent a "general exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). "The particularity requirement insures that a search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause." Id. The test is whether an executing officer reading the description in the warrant would reasonably know what items are to be seized. United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996). "In circumstances where detailed particularity is impossible, generic language is permissible if it particularizes the *types* of items to be seized." Id.

In this case the Warrant sufficiently limited the search to items containing child pornography and items that would show who used the computer, thus identifying the person who possessed the child pornography. It is clear from the Warrant what was to be searched and seized as set out fully in capital letters on page 2 of this R&R. Defendant's Motion to Suppress as to the particularity requirement should be denied.

Defendant's Detention and Statements

Det. McCartney testified at the Evidentiary Hearing that the Tactical Operations Unit entered the residence and secured it in preparation for the search. They encountered defendant in the basement and handcuffed him for their safety. They brought him outside

where he was contacted by Det. McCartney who identified himself, told him they were executing a search warrant for child pornography, removed the handcuffs and allowed defendant to put on a pair of pants over his boxer shorts. Det. McCartney asked defendant if he lived in the house and when defendant said "yes", Det. McCartney advised him of his Miranda rights as more fully set out above. Defendant said he understood his rights and agreed to speak to Det. McCartney. He asked what the Search Warrant was for and Det. McCartney again told him it was for child pornography. Defendant responded that all the child pornography was his. Det. McCartney told him to hold any further statements and asked him if he would come to the Detective Bureau for an interview. Det. McCartney specifically told him he was not under arrest and that the interview was voluntary. At Headquarters Det. McCartney re-advised defendant of his Miranda rights and defendant signed the Waiver form (Gov.Ex.2) as clearly shown in the CD of the interview (Gov.Ex.3).

Although defendant argues in his Motion that Det. McCartney lacked reasonable suspicion to seize defendant immediately upon meeting him, his Reply concedes that police may validly detain individuals on the premises during the execution of a search warrant for the purpose of safely and securely executing the search, citing Michigan v. Summers, 452 U.S. 692, 704-05 (1981). The government cites more recent authority: Muehler v. Mena, 544 U.S. 93, 98 (2005); United States v. Martinez-Cortes, 566 F.3d 767, 770 (8th Cir. 2009). It is clear that when Det. McCartney approached defendant he uncuffed him and advised him of his Miranda rights. The very brief detention of defendant by the Tactical Operations Unit was proper and lawful. The cases cited by defendant do not involve the execution of a search warrant which provides the officers with the limited authority to detain the occupants of the searched residence. Defendant's cases involve person who were handcuffed and involuntarily transported to the police department. Here Det. McCartney

explicitly told defendant he was not under arrest and defendant voluntarily accompanied him to Headquarters as fully confirmed on the CD.

To whatever extent defendant is claiming that Det. McCartney needed independent reasonable suspicion or even probable cause to advise him of his Miranda rights, the argument is without merit. The Supreme Court has rejected the argument that officers are required to have independent reasonable suspicion in order to question a person detained during the execution of a search warrant: "But the premise is faulty. We have 'held repeatedly that mere police questioning does not constitute a seizure.' [citations omitted]... as the Court of Appeals did not hold that the detention was prolonged by the questioning, there was no additional seizure within the meaning of the Fourth Amendment." Mueller, 544 U.S. at 97. In this case the Search Warrant was still being executed when Det. McCartney spoke with defendant. He advised him of his rights and explained that they were executing a search warrant. Mere police questioning does not constitute a seizure. In addition, Det. McCartney told defendant that he was not under arrest.

As noted when they reached Headquarters defendant was re-advised of his <u>Miranda</u> rights and signed the Waiver and spoke to Det. McCartney. For these reasons the defendant's Motion to Suppress Defendant's Statements should be denied.

Accordingly,

IT IS HEREBY RECOMMENDED that defendant's Motion to Suppress Evidence and Statements be DENIED. [Doc. 12]

The parties are advised that they have eleven (11) days in which to file written objections to this report and recommendation pursuant to 28 U.S.C. §636(b)(1), unless an

extension of time for good cause is obtained, and that failure to file timely objections may result in a waiver of the right to appeal questions of fact. See Thompson v. Nix, 897 F.2d 356 (8th Cir. 1990).

/s/Mary Ann L. Medler
MARY ANN L. MEDLER
UNITED STATES MAGISTRATE JUDGE

Dated this <u>15th</u> day of September, 2009.